(a) The Offeror will be evaluated on each proposed key personnel resume to determine:

- The demonstrated quality, relevance and applicability of the education and certifications of the individual proposed

- The demonstrated quality, relevance and applicability of the technical experience of the individual proposed, as it relates to the Key Personnel Qualifications (Attachment D).

(b) The Offeror's proposed labor categories and hours allocated to each category will be evaluated against the Statement of Work (SOW) to determine:

- Whether the labor categories identified provide the appropriate types of labor to allow for successful performance;

- Whether the hours associated with each labor category are appropriate and sufficient for the tasks required; and

- Whether the distribution of hours between the journeyman and senior levels of a specific labor category reflect an accurate understanding of the effort to be performed, as well as the stated expectation that FTEs will decrease over the period of performance.

- The demonstrated efficiency of the proposed organization in regards to consolidating similar functions or assigning multiple roles to individuals.

(c) The Offeror's proposed position descriptions for each non-key labor category will be evaluated for the demonstrated quality, relevance and applicability of education and technical experience requirements, the extent to which the category is necessary for successful performance, and the extent to which the proposed categories allow for consolidation of similar duties or roles.

(d) The Offeror's representative resumes for non-key labor categories will be evaluated to determine the quality, relevance and applicability of the demonstrated education, technical experience and its relationship to the proposed contract positions.

(e) The Offeror will be evaluated on its proposed plan for, and demonstrated ability to recruit, retain and replace both key and non-key personnel.

CRITERION 3: Past Performance

The Offeror will be evaluated with respect to performance in service contracting under existing and prior contracts of a similar type, scope, and complexity completed or in

progress during the past three (3) years. Performance information will be used for both responsibility determinations and as an evaluation factor against which Offeror's relative rankings will be compared to assure best value to the Government. The Government will focus on information that demonstrates overall quality performance relative to the size and complexity of the procurement under consideration. Assessment of the Offeror's past performance will be one means of evaluating both the credibility of the Offeror's proposal and the relative capability to meet performance requirements.
The Past Performance Assessment form provided as an attachment to the Request for Quotation will be used to collect this information. References other than those identified by the Offeror may be contacted by the Government with the information received used in evaluation of the Offeror's past performance. Information utilized shall be obtained from the references listed in the proposal and may also be obtained from other customers known to the Government. Information will also be considered regarding any significant subcontractors/team members and key personnel records.

The Offeror's past performance will be evaluated on:

(a) the degree to which the past and present performance evaluated adds to the Government's confidence in its ability to successfully deliver results to meet performance and customer satisfaction standards;

(b) the degree to which the past and present performance is of similar size, scope and complexity to that of the SOW;

(c) quality of performance: demonstrated compliance with contract requirements, specifications, accuracy of reports and standards of good workmanship (i.e., commonly accepted technical, professional, environmental, or safety and health standards);

(d) timeliness of performances – whether the Offeror met contract milestones/delivery dates, whether technical instruction deadlines were met, and adherence to contract schedules including contract administration;

(e) business relations – demonstrated ability to provide effective management of all activity needed, timely award and management of subcontracts, ability to timely respond to technical or administrative issues, responsiveness to inquiries, quality of problem identification and problem resolution, successful development and execution of corrective action plans, and overall professionalism and cooperation;

(f) cost control – demonstrated ability to operate within budget, the identification and use of cost efficiencies, relationship of negotiated costs to actual costs and the ability to provide current, accurate, and complete billing information;

(g) the Offeror's effectiveness in forecasting, managing, and controlling contract costs, including reporting and analyzing variances; and

(h) overall customer satisfaction.

CRITERION 4: Business Management Approach

The Offeror will be evaluated on its proposed management approach for accomplishing the work to be performed, including a demonstrated understanding of the contract requirements and plan for completing these requirements in a timely and high quality manner. This will include assessing:

(a) Effectiveness and appropriateness of its proposed organizational structure for performance of the contract and its processes for resolving problems, decision making, and resource commitment, including the lines of program management authority and the degree of autonomy, accountability, decision-making, and delegation authority vested in the Program Manager.

(b) Demonstrated corporate commitment and application of corporate policies and procedures to manage and perform the SOW.

(c) The proposed teaming agreements and plan for management of team members or subcontractors.

(d) Team composition, with a focus on evaluating the combined strength of the team to leverage commercial best practices in providing innovative and effective program management solutions.

(e) The degree to which the management structure and approach foster an open Government-Contractor relationship that leverages shared performance goals/objectives and enhances confidence, credibility, and trust.

(f) The Offeror's cost management/containment processes to be implemented in the execution of the contract; and

(g) The Offeror's plan for efficiency in staffing, including the extent to which multiple roles are assigned to individual labor categories or personnel, or to which similar duties are consolidated into a specific labor category.

Price Evaluation Factor

The Offeror's price and labor mix will be evaluated to determine if the proposed price is realistic and reasonable to effectively perform the SOW requirements. The Government-evaluated price will be used to determine the best value trade-off for source selection.

Other Information

All expenses related to the submission of this proposal and document preparation will be the sole responsibility of the offeror. Late proposals, as defined in FAR 52.215-1, shall be rejected.

Sincerely,

/ s /
Lynnette A. Desorcie
Contracting Officer
Office of Naval Research

The following are attached to this document:

Attachment A, Statement of Work
Attachment B, Special Terms and Conditions
Attachment C, Key Personnel Qualifications
Attachment D, Performance Standards
Attachment E, Contract Security Classification Specification (DD Form 254)
Attachment F, Mission Essential Contractor Services
Attachment 1, Past Performance Questionnaire
Attachment 2, Non-Disclosure Agreement Regarding Contractor Support for the Office of Naval Research

ATTACHMENT A – STATEMENT OF WORK

1.0 BACKGROUND

The Office of Naval Research (ONR) needs all of its legacy Command, Control, Communications, and Computer (C4) support (described in Attachment A-1, Contractor Support Requirements for Legacy Applications) in one enterprise program that will support planning, program management, integration, operation, and maintenance of the communications, computer networks, and software applications. ONR needs to improve its ability to easily extract data and provide information for decision making. The objective of this Contract is to assist ONR in gaining efficiencies to establish a world-class network operation while fully supporting ONR's business processes. This is intended to reshape how ONR manages its business processes and focuses on streamlining business processes supported by enabling Information Technology (IT) that will make ONR's business processes more efficient. The end state is the divestment of legacy systems (See Attachment A-1), a reduction of the current legacy network and a reengineering/transformation of its remaining components into a Navy "excepted" network supporting the research, science and technology requirements of ONR, and a successful, seamless transition to Navy Marine Corps Intranet (NMCI) and Navy Enterprise Resource Planning (ERP).

ONR currently operates a legacy network that supports the delivery of IT services such as email, Blackberry services, web hosting, applications support, video teleconferencing, and Knowledge Management (KM). ONR also employs services provided by the NMCI environment such as Seat Management capabilities for PCs, phones, and printers. The overall goal of ONR is to move as many services as possible to NMCI, while preparing itself for a transition from its legacy and NMCI infrastructure to Navy's Next Generation (NGEN) IT services contract and Navy ERP implementation scheduled for 2012. ONR 's focus is to maintain maximum flexibility while providing new methods and approaches allowing ONR Command Information Officer (CIO) to conduct business more efficiently and cost effectively. In addition, a supporting IT architecture must be maintained that is both flexible and adaptable to changes in technology standards (both government and industry) and supports the research, science and technology requirements of the ONR staff. ONR requires a common data repository that ensures the availability of valuable organizational intelligence to provide ONR's leadership with predictive decision-making and actionable information. The use of a commercially available "software as a service" solution for data base/application remote hosting, application management, and disaster recovery will continue to be explored as a method to divest ONR of disparate legacy hardware and sustainment costs and allow the system to operate at a less expensive rate while ensuring a high availability rate.

ONR uses a methodology that takes advantage of ever changing and developing business processes. Processes cross and flow between multiple organizations, which includes ONR's internal and external employees, and/or customers. The contractor shall develop and test improvements and implement electronic business process solutions. As ONR transitions into Navy ERP, it is expected that ONR's investment in Naval Research Information System (NAVRIS)(Oracle eBusiness Suite) will decline and transition toward Navy ERP, NGEN and KM solutions.

In addition to this solicitation ONR is also working on an internal solicitation for an Independent Validation and Verification (IV&V) contract. This requirement will include a small number of resources to support the government team in project management oversight duties and will interface with the ONR support contractor.

2.0 SCOPE

The Contractor shall provide IT support services for the C4 systems that support ONR Headquarters in Arlington, Virginia (approximately 1,100 users); as well as ONR field locations in Boston, Atlanta, Seattle, San Diego, and Chicago (approximately 90 field location users); and ONR Global (ONRG) (approximately 35 users) in Singapore, London, Tokyo, Santiago, and Prague, as required. The scope of this contract is to provide services for program management, business process improvement, and operational support services to ONR as it further develops its emerging business processes supported by state-of-the-art information technologies. The goal is to ensure full exploitation of those processes and technologies and to ensure that business processes are continually reviewed to identify where improvement opportunities exist. This includes all ONR networks, Nonsecure Internet Protocol Router Network (NIPRNET), Defense Research Enterprise Network (DREN)), Secret Internet Protocol Router Network (SIPRNET) and applications and capabilities (e.g., NAVRIS, Contract Writing Tool, Intellectual Property Management Information System (IPMIS), Business Intelligence (BI), AwardWeb, PRISM).

3.0 TASK PERFORMANCE

3.1 TASK AREA 1 – CONTRACT MANAGEMENT SUPPORT

3.1.1 Program Management

The Contractor's Program Manager shall be the focal point for all issues in this program and shall keep the Government Contracting Office Contract Officer and Contract Officer Representative (COR), as well as the ONR Technical Point of Contact (TPOC) and CIO Leadership, fully informed both verbally and in writing. The Contractor shall provide a method for senior ONR personnel to receive program level information and allow them to drill down to have visibility into individual metrics to assess problem areas.

The Contractor shall provide program management support that includes the management and oversight of all activities performed by the contractor personnel, including subcontractors, to satisfy the requirements identified in this contract. The Contractor shall effectively and efficiently manage project cost, schedule and performance utilizing integrated program management processes across all aspects of the contract tasks and activities; and shall identify opportunities for potential cost savings such as crossed trained personnel, to provide the best value to the Government. The contractor shall provide contract management, transition planning, quality assurance, metrics management, project control, risk management, lessons learned, cost management,

integration and configuration management, communications management (including telecommunications) and time management.

The contractor should follow best practices from the Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK).

The Contractor shall provide complete program, financial, technical, and contractor personnel management support as depicted below that will fully integrate, manage, control, and document all phases of the contract requirements.

- Program Management
  - Schedules and Timeliness
  - Responsive to Customer Needs
  - Documentation
  - Project Management with task project plan as required
  - Process Improvement
  - Emerging Technologies / Innovation
  - Continuity of Operations
  - Root cause analysis.
  - Business Analysis
  - Integrated Master Schedule
- Personnel Management
  - Turnover management
  - Training and Staff Development
  - Coverage/Deployment
  - Personnel Resource Planning.
- Financial Management
  - Accurate, Clear, and Timely Invoicing
  - Cost Containment
  - Trends Analysis
  - Cost Forecasting
- Technical Effectiveness
  - Quality and Productivity Assessment
  - Implementation and integration of new hardware, software, procedures, and technology refresh procedures
  - Routine Operation and Maintenance
  - Technological Innovations

Within ten (10) working days of the award of this contract, the Contractor shall participate in a Contract Kick-Off Meeting. The Government will conduct the contract Kick-Off Meeting with ONR personnel and other Government representatives to review and discuss contract administrative matters, security requirements, project transition, Government Furnished Information/Government Furnished Materials/Government Furnished Equipment (GFI/GFM/GFE), the milestone schedule, review cycles, and invoicing. The Government will hold this meeting at the government site and coordinate an agenda with the Contractor.

The Contractor shall adhere to the guidelines outlined in DoD 8570.1 "Information Assurance Training, Certification, and Workforce Management" to determine the security IAM/IAT access level requirements for all personnel. The COR and the ONR Information Assurance Manager (IAM) or a designated representative will review Information Assurance Work Force (IAWF) personnel certifications for approval before the personnel can begin work. The Government reserves the right to have any employee who does not meet this requirement removed from the contract.

Throughout the course of the contract, ONR will provide to the contractor opportunities to develop and implement IT enhancements that are considered new functionality and beyond the core contract requirements. The contractor shall provide to the ONR TPOC a project plan identifying the project objective, scope, current and out-year costs, return on investment, approach, estimated date of completion, resource requirements, and alternatives considered. Upon approval of the project plan by the ONR TPOC, the contractor shall include the project in the Program Management Plan (PMP) for tracking and oversight and follow the guidelines identified for software development and maintenance.

3.1.1.1 Prepare Program Management Plan (PMP)

The Contractor shall develop, maintain, update, and execute throughout the contract period of performance a PMP and shall use it as a foundation for information and resource management planning for successful schedule, technical, and cost performance. DoD Directive 8115.1 Information Technology Portfolio Management, dated October 10, 2005, mandates that agencies manage IT investments as portfolios, with a selective requirement down to the task level. The contractor shall support ONR in the management of these portfolios. ONR currently is evaluating several automated tools to support the portfolio management process.

The PMP shall describe the contractor's organization, resources, processes, and management controls that will be deployed. The PMP shall define the proposed organizational structure (including responsibilities and reporting structure), how personnel will be assigned throughout the contractual period, and how the proposed project team will interface with both the contractor's corporate structure and the Government command structure. The PMP shall describe the contractor's proposed recruiting/hiring program for staffing the contract with qualified personnel over the period of performance. The PMP shall define policies and procedures for managing and directing the effort for productivity, quality, cost control, and early identification and resolution of problems. The PMP shall include milestones, tasks, and subtasks required in this contract. The PMP shall also identify a series of metrics that will be used to track the progress of and ensure the goals of the PMP and the tasks of this contract are being met. The PMP shall provide for a Work Breakdown Structure (WBS) in accordance with MIL-HDBK-881, and data item description DI-MGMT-81334B, and associated responsibilities and partnerships between Government organizations by which the contractor shall manage all work.

The PMP shall address all areas from Task C.3.1.1 Program Management and include the following documentation that comprises the PMP.

- Contract Management Plan (COMP).
- Contingency Plans.
- Quality Control Plan (QCP).
- Risk Management Plan.
- Task Management Plan
- Staffing Plan
- Work Breakdown Structure (WBS)

The Contractor shall keep the PMP up-to-date, have the plan and metrics accessible electronically at any time on ONR's website with ONR's .mil domain, and be prepared to brief any PMP content to the Government on 24 hours notice. The contractor shall work from a Government approved PMP. The contractor shall use the PMP as a foundation for the Status Report.

3.1.1.2 Participate in Status Meetings

The Contractor shall participate in weekly status meetings to review current and planned activities for the major task areas. Status briefs shall include project level briefings with contractor personnel and government process owners, and an overview level status briefing by the Contractor Program Manager with the ONR TPOC and Code 06 Branch Directors (Operations, Applications, Web Services, Information Assurance, Enterprise Architecture, IT Compliance, Communications and Budget and Finance). The Contractor shall prepare an "Activity Report" at least one workday prior to the Status Meeting that details the results and planned actions for the Contractor's project teams. Typical topics may include the project status, stoplight charts, status of services, maintenance efforts, and planned acquisitions and changes/updates to the PMP.

3.1.1.3 Financial Status Report

The Contractor shall distribute a Financial Status Report once a month for all work efforts. The Financial Status Report shall include:

- Administrative Information
  - Contract Number
  - Contractor Name, PM name and contact information
  - Date of Award
  - Period of Performance
  - Contract Award Amount
- Current Financial Information
  - All hours and costs broken out by task and CLIN for the current reporting period
  - Cost cumulative for the Contract

The Transition-Out plan shall facilitate the accomplishment of a seamless transition from the incumbent to incoming Contractor/Government personnel at the expiration of the period of performance. The Contractor shall provide a Transition-Out Plan NLT 90 days prior to expiration of the contract (or within 30 days after Government notification that an option will not be exercised). The Contractor shall identify how it would coordinate with the incumbent and or Government personnel to transfer knowledge.

The Contractor's Transition-Out Plan shall contain the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Inventory of hardware and software
- Status of ongoing technical initiatives, including risk identification and analysis
- Appropriate Contractor-to-Contractor coordination to ensure a seamless transition
- Transition of personnel
- Schedules and milestones
- Actions required of the Government
- Methods to use to establish and maintain effective communication with the incoming Contractor/Government personnel for the period of the transition

3.2 TASK AREA 2 - SYSTEMS SUPPORT

3.2.1 Systems Support – The Contractor shall provide management of ONR's legacy/"excepted" network, software applications, and customer support. Contractor shall provide support that is forward-thinking, consistent with government standards, efficient, and leverages IT to attain ONR's mission goals and objectives. To support these challenges, Contractor shall provide a plan and strategy for delivering timely and cost effective IT services using an Information Technology Infrastructure Library (ITIL) Framework that integrates all phases of the IT Service Life-Cycle including information assurance. The Contractor shall provide the strategy and plan for ITIL implementation to the COR and ONR TPOC for comment and implementation after final approval of the plan from the government.

The Contractor shall provide an initial assessment of the ONR Legacy Network to determine the overall health of the environment and a projected plan for infrastructure replacement and/or major upgrades in order to meet service level agreements identified in the contract.

All Information Technology Systems or software/application development, modification or support shall be performed in accordance with the Clinger/Cohen Act, Defense Business Transformation Agency (BTA) guidance (formerly Business Management Modernization Program (BMMP)), Navy Marine Corps Internet (NMCI), Enterprise Architecture BEA 7.0 Compliance Guidelines, DON/S&T Functional Area Manager (FAM) Policies and Guidance, DITPR-DON/ Network and Server Registration, DON and

Naval Network Warfare Command (NNWC) Directives and Instructions and Web Enablement mandates.

3.2.1.1 Legacy Network Engineering Maintenance Support

The Contractor shall establish and manage a comprehensive Legacy Network Maintenance Program that includes installations, connections, access control, configurations and inventory of ONR Headquarters and Field Office legacy network devices, including firewalls, routers, servers, cabling, and other network components. The Contractor shall provide comprehensive network and system support, including:

- Baseline Inventory and periodic inventories of network hardware and software;
- Network Policies, procedures, and guidance;
- Network implementation;
- Configuration Management Process;
- Scheduled maintenance;
- Unscheduled maintenance;
- Planned and integrated logistics support for existing system components;
- Integration of new technology;
- Technical Knowledge Database;
- Network Account Management; and
- Information Assurance (IA) (to include compliance with DoD IA mandates, directives and configuration standards).

The ONR strategy for information technology sustainment is to streamline capabilities to be more cost effective and to get IT resources aligned with the policy, guidelines, and compliancy standards of the Department of the Navy (DON). NMCI, NGEN (the replacement for NMCI), and the mandate to consolidate all public accessible websites with hosting at a DISA Defense Enterprise Computing Center (DECC) per NAVADMIN 08/061, are a few examples of Navy Policy that will drive the network architecture to reduce the information technology footprint at ONR and costs. Relevant policy guidance such as the DoD-Wide Digital Signature Interoperability Policy dated 5 May 2006, DoD Clinger-Cohen Act Compliance Policy dated 8 March 2002, and Department of Navy's Naval Networking Environment (NNE) Strategy Definition and Scope dated 13 May 2008 can be found on the Department of the Navy, Command Information Officer Website at http://www.doncio.navy.mil/policy.aspx.

The Contractor shall:

- Provide (and implement upon Government approval) a Network Strategy Plan that provides short term (2 years) and long term (5 years) goals depending on the DON and government policies and guidelines effecting transition and compliance activities. Examples of short term goals would include further migration to NMCI for email, email storage, blackberry support, data migration and applications migration. Some long term goals would include the reduction of the

size of the existing legacy network and its transformation into a Navy "excepted" network supporting the research, science and technology requirements; the replacement of NMCI with NGEN and DISA DECC web consolidation and hosting migration efforts-taking advantage of existing DoD, DON, and Federal IT resources.

- Provide operational support and maintain the ONR legacy network 7 days a week, 365 days per year. Onsite support will be provided Monday through Friday excluding government holidays, from 0600 through 1800. During specified off-shift hours (Monday through Friday 1800 through 0600, weekends (which are Friday 1800 thru Monday 0600), and holidays, the Contractor shall be "on call" with a 2 hour response time to provide assistance when necessary.
- Perform legacy network hardware, software, and firmware installations, upgrades, maintenance, and troubleshooting on a mutually agreed upon schedule. All agreed upon schedules shall be available for review during weekly network status meetings. Configuration Management must be practiced and all Configuration Items must be identified according to configuration of system. Before new projects are implemented by the engineers, they must use Network Analysis, Critical Path Analysis (CPA), or the American Program Evaluation and Review Technique (PERT) process to assist in producing their schedules and show effort required.
- Maintain a knowledge base database of incidents and problems showing steps taken to solve each issue.
- Maintain an inventory of all configurations of network devices including servers, switches, routers, firewalls, etc. These listing shall be maintained in a secure environment and available to ONR personnel upon request.
- Perform network administration to include design, testing, installation, operation, maintenance, and management of ONR networks.
- Periodically utilize vulnerability identification tools to determine whether systems are correctly designed and configured, and whether all necessary software patches and fixes are applied.
- Maintain and refine procedures and processes to detect errors and inconsistencies in the computer-resident privileges using by computer and network access control systems, such as a procedure to identify user-ids that have not been used in 90 days.
- Assign and distribute user-ids and initial passwords to authorized users according to established ONR policies and procedures; and assure that accesses are removed for users who have left ONR; and that users who have switched jobs receive only the privileges needed to perform their new jobs.
- Disable user accounts and/or privileges immediately in those events where a user is found guilty of a major crime, has seriously violated internal ONR policy, or has left ONR (especially important for duress terminations).

- Securely preserve all records indicating changes made to access control lists to facilitate problem resolution efforts, security incident investigations, and disciplinary actions.
- Periodically review access control logs and reports to ensure that the network is working properly and that no unauthorized activity is taking place.
- Provide contractor-sponsored training annually for all contractor network engineering staff members to maintain their job related skills and performance levels as well as their network certification criteria.
- Implement software and hardware upgrades, repairs, and replacements required to maintain the ONR LAN and WAN and its associated subsystems at peak operating efficiency. Provide metrics on mean time to repair and mean time between failures.
- Implement and track all patches, upgrades, enhancements, and/or bug fixes to servers, firewalls, web commerce servers, etc. through various methods; and evaluate and determine whether the change will cause incompatibility problems, system crashes, system response time degradation, and/or other operational problems before installing any change. Ensure Information Assurance Manager (IAM) and Configuration Management Board (CMB) approval. Recommend during weekly network and/or CMB meetings, which patches to implement on the LAN.
- Periodically run software that inventories the hardware resident on ONR legacy network to assure that hardware is still operational, has not been stolen, or has not been redeployed elsewhere without permission.
- Maintain an inventory of all software and hardware associated with the ONR Legacy network, including software components on each server. Inventory shall include equipment description, manufacturer, model number, serial number, date of purchase, inventory tag number and purchase price and in the case of software the quantity of each license purchased.
- Maintain an inventory of all NMCI software and hardware. Inventory shall be maintained by machine and include equipment description, manufacturer, model number, serial number, date of purchase, NMCI inventory asset tag number and the software installed on each machine.
- Re-configure and reinstall operating systems and other security systems when there is clear evidence that the security of a system has been compromised.
- Operate and maintain Microsoft Exchange servers, Simple Mail Tranfer Protocol (SMTP) gateways, email and remote clients, until transitioned to NMCI. After that, provide help desk assistance where possible for these items.
- Perform installations of new and upgraded software applications and operating system software on the LAN servers in accordance with the manufacturer's specifications.
- Re-configure and reinstall operating systems and other Internet related security

systems according to established policies and procedures whenever there is credible reason to believe that the security of a system has been compromised.

- Configure all hardware (servers, switches, routers, etc) and software (operating systems (OS), databases, applications, etc) to meet the Security Technical Implementation Guide (STIG) environment mandated for each by the Defense Information System Agency (DISA).
- Configure and maintain IBM and Linux servers as well as other Intel based servers, SMART array controllers, Redundant Array of Independent Disks (RAID) level configurations, hard drives, and memory expansions.
- Maintain all ONR legacy cabling and cabling components. Install new cabling as required to support new node installations and network equipment moves. Disconnect and connect microcomputers, printers, and servers connected to NMCI and legacy networks, coordinating with the Helpdesk, for all network connected equipment moves. Ensure that all Government Furnished Material (GFM) network diagrams are maintained for all new or modified network-wiring installations and that all cabling is labeled with a unique designator to identify its location relative to building floor and room number.
- Perform legacy hardware installation, problem determination, troubleshooting, and maintenance and support for all existing and new LAN cabling and cabling components, i.e., switches, routers, boundary routers, and Channel Service Unit/Data Service Unit (CSU/DSU) systems. The Contractor shall provide support based on the standards associated with RS-232, V.35, Ethernet (Fast and Gigabit), unshielded twisted pair (UTP) and related cabling systems including the installation of cables, connectors, wall outlets, patch panels, and the troubleshooting of cabling problems using GFM cable testers.
- Ensure all network devices are labeled for quick identification.
- Install, configure, and maintain backup systems for backup and disaster recovery capability. Ensure that backup processes are running properly, data can be fully restored, and backup processes create appropriate operational logs.
- Maintain network communications throughout the legacy network to external networks and interfaces required for ONR operations, such as to:
    - Internet
    - Defense Enterprise Computer Centers (DECC)
    - Defense Research Engineering Network (DREN) to the regional field offices via point to point and Internet/VPN tunneling
    - STARS, a point-to-point solution using IBM's Web Sphere MQ Series software to interface with the Navy Defense Finance and Accounting Service (DFAS) Official Accounting System located in Mechanicsburg, PA.
    - NIPRNET circuit and router configurations for the remote hosting facility for ONR's mission critical applications.

  - CITRIX connectivity to DON ERP systems.
  - SIPRNET NMCI connection.

- Remotely maintain ONR Regional Office network communications and, when required, contractor shall visit field offices to install, replace or upgrade software and/or hardware, troubleshoot, and/or conduct training.
- Attend government/contractor weekly network meetings to discuss unresolved issues and priorities. The agenda shall include all unresolved network related problems, planned upgrades, enhancements, and/or changes (excluding Helpdesk-related open calls and issues).
- Maintain and support World Wide Web (WWW) servers, a Secure File Transfer Protocol (SFTP) server, and a CD-ROM server. Provide support for FTP, Telnet, TN 3270, and Digital Communications Associates (DCA) terminal emulator software (i.e., Win Zip for Windows).
- Install, maintain, document, monitor and troubleshoot Internet IP filtering routers, Intrusion Protection System (IPS) and Internet firewall systems in compliance with applicable directives. The Contractor shall maintain and archive with auditing access provided to the Information Assurance Manager (IAM); and report abnormalities to the IAM as soon as possible (no later than 1 hour after discovery).
- Document and maintain all LAN and WAN baselines and enhancements, in accordance with configuration management practices.
- Assist the government in defining and maintaining IT portfolio management: the "as-is" and creation of the "to-be" ONR enterprise architecture that will detail the vision, scope and objectives, processes, planning methodology, work-plan, budgets and computer resources as required by the Clinger-Cohen Act and DoD architecture framework (DODAF). This shall include the development of technical data, data and system functions/component taxonomies and anthologies, network topologies, and data flow diagrams.
- Develop, update, and maintain detailed network logical and physical connection network diagrams and documentation. This will include technical data, data and system functions, Group policies (GPOs), privileged accounts, and network topologies. In addition, there should be a separate mapping of GPOs along with detail describing each policy. The same should be followed for each privileged account.
- Identify, install, and maintain a network application monitoring system (network analyzer(s), etc.) that, at a minimum, will enable the contractor and government the ability to provide for capacity planning (future router, switch, storage, bandwidth requirements, etc pursuant to trend analysis and/or proposed designs), foresight (what-if-analysis, etc.), and general network troubleshooting.
- Identify, install and maintain a monitoring system that enables the contractor and government to determine if software applications are operating correctly.

- Establish an Information Assurance Officer(s) (IAO) for each system and major application as identified by the ONR Information Assurance Manager (IAM), The IAO is responsible to the IAM for ensuring the appropriate operational IA posture is maintained for their system or application.
- Manage all configurations and new installations. All changes shall be documented for the Configuration Management Specialist (CMS). Contractor shall analyze to determine the impact on security, any change in threat, vulnerability, configuration, hardware, software, connectivity or other modification. The IAM/CMS/IAO will identify changes that will require a written risk assessment, along with required DIACAP documentation to update the accreditation of the system.
- Install, maintain, configure and troubleshoot routers, switches, and concentrators. ONR currently utilizes Cisco routers, Cisco switches, and Cisco concentrators.
- Predetermine traffic routing to support load balancing and make changes as needed for peak performance.
- Perform frequency allocation, route analytics, bandwidth management and performance management.
- Implement Internet Protocol IP addressing and routing.
- Practice active Fault Management by using tools such as Time Domain Reflectometers (TDRs), cable scanners, network monitors, LAN probes, protocol analyzers, and sniffers.
- Perform preventive maintenance on all supported network devices.
- Maintain proper accountability of all network infrastructure assets.
- Develop, maintain, manage and integrate networked systems to provide robust and secure day-to-day headquarters network operations.
- Provide network systems administration for the ONR legacy networks.
- Implement modifications to network equipment, software, and facilities to sustain peak network operations; and provide network(s) maintenance support and computer and network installations.
- Monitor computer and network activity including system load, response time, available disk space, and users activities to ensure that all activities are in keeping with ONR CIO intentions.
- Manage and maintain a master station log and shift change procedures to ensure proper information flow across the shifts and during personnel changes. Procedures shall include passwords to servers, applications, etc.
- Provide technical assistance to ensure all ADP hardware purchased by ONR is in compliance with the most current approved "Standard Configuration" and IAW with Section 4.17 of DoDD 8500.1 which outlines the requirement for all IA and IA-enabled IT hardware, firmware, and software components and products

incorporated into DoD information systems to comply with specified DoD evaluations and validations .

- Provide aggressive network security management through direct support of Computer Network Defense (CND) initiatives to include review of network security scans and intrusion detection reports and implementation of security fixes, upgrades and applications.
- Provide in-depth technical support services to the Office of the CIO Management to help them understand the systems software issues associated with achieving certain performance, reliability, and security goals.
- Maintain accurate records reflecting current and historical configuration settings and the justification for these settings.
- Inform the System IAO and Information Assurance Manager (IAM) of improper configuration, dangerous internal practices, and other matters that might jeopardize the security of production computer systems, to the extent that these matters can be identified in the course of performing duties.
- Run auto-detection software routines to discover prohibited software that can be used to compromise systems security, and then remove such software.
- Participate on, cooperate with, an Incident Response Team that responds to various security incidents such as denial of service attacks, and virus infestation
- Provide oversight and report to management on network security health and status.
- Provide engineering and technical expertise on all legacy data network issues within ONR, including interoperability, standards, compliance, information assurance, communications, and connectivity; and provide bi-monthly reports on performance to the ONR TPOC.
- Create and maintain technical documentation for each system.
- Assess, recommend, and (at Government direction) execute a COOP strategy for ONR legacy environment.
- Provide in-depth engineering and technical expertise to support the planning and migration of ONR legacy email, data and applications to NMCI, DISA DECC or other remote hosting facility. This expertise shall include the identification of issues to include but not limited to the dependencies associated with email, applications and data on each other or other systems, as well as the identification of organizational dependencies such as ONR Global and their requirements to access data and applications proposed to move to NMCI.
- Provide technical and support expertise to ONR staff concerning the use of Navy ERP systems.

3.2.1.2 Engineering, Test, Analysis, Development and Integration Lab

The lab is intended for the engineering, testing, analysis and integrating into production of both technical solutions that meet ONR strategies and business process improvements that are IT-enabled. The contractor shall design and implement the laboratory/ development system for the Microsoft Windows based environment at ONR. The lab will be located on a segment of the ONR legacy network and will be designated as a DEV/MOD segment and implemented with government furnished equipment or contractor provided equipment. The Government will make this decision based on the evaluation of alternative solutions. The design of the lab must comply with all DoD IA and architecture requirements mandated for the current ONR production environment.

The Contractor shall test all hardware, software, and network configuration upgrades, additions, and revisions in the laboratory for Government approval before implementation. This includes downward-directed systems underwritten by the Department of the Navy or other Government agencies. The CIO also relies on laboratory testing and recommendations before concurring on any hardware or software additions or upgrades to the Command networks.

The Contractor shall:

- Provide information systems engineering, testing, analysis, and integration as well as associated written reports for ONR strategies. Before new projects are implemented by the engineers they are to use Network Analysis, Critical Path Analysis (CPA), or the Program Evaluation and Review Technique (PERT) process to assist in producing their schedules and show effort required.
- Perform broad network and computer engineering tasks.
- Apply expertise on multiple aspects of computer network architectures on complex, cross-connected systems.
- Test all software patches, upgrades, Information Assurance Vulnerability Management (IAVM) and Computer Tasking Order (CTO) Directives solutions, new configurations and products, in the lab prior to determine their effects on the ONR production environment and recommend and develop solutions to any identified issues prior to deployment.

3.2.1.3 Visual Information Services and Audio Support Service

The Contractor shall support Video Teleconferencing (VTC) and Audio/Visual (AV) systems. The Contractor shall provide state of the art, networked visual information services for ONR Headquarters and its meeting and conference facilities. This shall include set ups, adjustments, and operation of audio/visual equipment and support for the VTC and AV equipment for ONR virtual employees.

The Contractor shall:

- Perform weekly system checks in the ONR HQ Management Information Center (MIC) located on the 14th Floor of the ONR Headquarters and communicate

deficiencies and required repairs to the ONR Program Officer and a third party maintenance contractor. Section J, Attachment A-2 contains a list of equipment the contractor shall manage.

- Maintain and support video teleconference hardware.
- Provide remote access solutions using Integrated Services Digital Network (ISDN), Primary Rate Interface (PRn) and/or Basic Rate Interface (BRn) and provide recommendations during weekly network status meetings.
- Manage VTC phone line additions, changes and moves.
- Manage requirements for telephones, voice over IP (VOIP) to include Unity and Call Manager administration, security, and general server maintenance.
- Provide configuration management of telephone lines, VOIP server equipment, and Direct Inward Dialing (DID) numbers per government approved practice and manner.
- Install, configure, maintain and troubleshoot ISDN video teleconferencing equipment and systems that include:
    - Wireless LAN Access
    - Support for telecommuters
- Recommend changes to ONR procedures and policies for video teleconference/audio visual support.
- Recommend cost savings for this support.
- Engineer, operate and maintain suites of VTC and AV hardware and software. This shall include the performance of routine preventative maintenance support on all AV and VTC assets as specified by the manufacturer or local operating instructions.
- Schedule, coordinate, and administer VTC and AV sessions.
- Recommend and implement upgrades to the VTC and AV systems at least annually and incorporate approved upgrades.
- Engineer connectivity to other locations and equipment, including ONR audio/visual systems.
- Train personnel on AV and VTC equipment.
- Support cable and satellite television service requests.
- Validate cable and satellite billing.
- Cover AV/VTC events outside normal operational hours.
- Ensure all configurations and operations meet DISA PC Communications Client STIG and DISA VTC STIG

3.2.1.4 JWICS Systems Support

The contractor shall provide all necessary personnel resources to manage, operate, maintain, and support Joint Worldwide Intelligence Communications System (JWICS) systems in the Secure Compartmented Information Facility (SCIF) at ONR. JWICS is a TS/SCI computer network and will require that all personnel supporting this effort are cleared for access at the TS/SCI level.

The contractor shall perform the following functions:

- Operate, support, and maintain the JWICS systems during normal business hours. During normal business hours, a response time of 1 hour, on the average, is required for problem resolution.
- Provide technical assistance and support, both via telephone and workstation site, in all aspects of hardware and software operation and use for all ONR government (includes IPAs and detailees) and contractor employees.
- Troubleshoot workstations, peripheral devices, printers, and/or the network connection to determine the extent of repairs required, if any. If a hardware repair is required, refer the problem to the JWICS TPOC for resolution by the contract maintenance vendor.
- Maintain detailed records of all helpdesk trouble calls and assistance provided to users. To the extent possible without divulging classified information, records shall include all open and closed calls to date, name of technician assigned to each call, the date and time the call was opened, and corrective action taken. The Government is currently using Remedy helpdesk software.
- Install, configure, maintain, and troubleshoot JWICS video teleconferencing equipment and systems.
- Provide support for the JWICS video conferencing operations. Support shall include scheduling and pre-appointment setup of available resources. Provide custody control of minor property for use with the video teleconferencing system. Coordinate with government supplied sources for repair/maintenance of equipment. Equipment will include all devices and wiring backbone supporting this capability.
- Support the containment, cleanup, and reporting of the spillage of classified materials onto SIPRNET or unclassified networks.
- Provide in-depth technical advice for investigations of information security incidents including internal frauds, hacker break-ins, and system outages.
- Assist with the documentation of information security incidents as well as the analysis of the circumstances enabling or permitting these same incidents to take place.

3.2.2 Customer Services Support

3.2.2.1 Service Desk and Customer Support Center

The contractor shall provide customer support for personnel at ONR Headquarters and field site locations for unclassified and classified systems and shall provide value-added services through a single point of contact delivery model. Support shall include helping users use IT products and services such as ONR's legacy network, commercial-off-the-shelf productivity tools, such as MS Office, Opentext Livelink; and ONR's mission critical software applications. For the last 9 months ONR has observed an average of 1030 tickets open per month, with peak activity during the 3rd and 4rth quarters of the fiscal year. The mission critical software applications are:

- Naval Research Information System (NAVRIS) (Oracle eBusiness Suite)
- Science and Technology (S&T) Toolkit
- Intellectual Property Management Information System (IPMIS)
- AwardWeb
- Naval Science Award Program
- Electronic Proposal
- Official PassPort
- Defense Travel System (DTS)
- Standard Labor Data Collection and Distribution Application (SLDCADA)
- Defense Civilian Personnel Data System (DCPDS)
- Business Intelligence Dashboards
- Navy Marine Corps Intranet (NMCI) Gold Disk

The Service Desk shall serve as the liaison between ONR users and system engineering network and development teams. The Contractor shall identify, research, and resolve technical problems as well as respond to telephone calls, automated Service Desk requests, email, and other requests for technical support. ONR currently uses Remedy to manage Service Desk Administration.

The Contractor shall establish and operate a walk-in Customer Support Center (One Desk) on Government Business Days from 0600-1800 Eastern Time at ONR Headquarters in Arlington, VA. During specified off-shift hours (Monday thru Friday 1800-0600 and weekends and holidays), the contractor shall be on-call to provide assistance when notified via pager. The Contractor shall:

- Provide incident management for all enterprise incidents and timely return to service requirements for users and the enterprise. The contractor shall report status on incidents to users and develop an incident status on-line capability.
- Promptly document and create trouble tickets for all reports of information systems problems, including system unavailability, unacceptable response time,

unauthorized access, missing files, and virus infections; and immediately notify management if an information security incident meets escalation criteria.

- Provide support via phone, email, Web, or Walk-in.
- Support new customers with the laptop configuration requirements including drive mappings, email setups, and PST (Personal Storage) builds.
- Provide support to end users on a variety of IT issues.
- Identify, research, and resolve technical problems.
- Assist and coordinate in the incident management process to include identifying, researching, and resolving technical problems.
- Respond to telephone calls, e-mail, and in-person requests for technical support.
- Resolve, track, and monitor incidents to ensure a timely resolution.
- Recommend a methodology to better manage Customer Service Desk support services within 30 days of contract transition that provides the Government with metrics showing:
    - Quality of services provided.
    - Responsiveness to customer needs.
    - Proactive and continuous strategy to reduce calls and improve service.
    - Customer satisfaction

3.2.2.2 NMCI Assistant Contract Technical Representative (ACTR) Support

The Contractor shall provide direct support to the Contract Technical Representative (CTR) for all NMCI-related functions; from pre-transition through cutover and continuing through post-transition. The Contractor shall collect and maintain documentation of all phases of NMCI, including deployment, service acceptance and other transition activities, cutover issues; and expansion and changing of services post-transition. Act as liaison between ONR-based personnel and other agencies on NMCI related issues. The Enterprise Information Technology Service Management System (EITSMS) encompasses CDR, eMarketplace (eMp), ISF Tools, NMCI Enterprise Tool (NET), Requirements to Award Process Tool (RAP Tool) and Service Request eForms (SReForm).

The Contractor shall provide the following support:

Service Ordering

- Prepare and submit the necessary documents to request new services.
- Prepare and submit Move, Add, Change (MAC) documents as required.

- Process all information or documentation necessary to obtain, change or remove accounts, hardware, software and other services for all ONR-based employees.
- Create and process routine and non-routine service orders.
- Coordinate the specific deployment schedule of all services
- Communicate special user deployment instructions to HP/EDS.

Help Desk

- Provide information on Trouble Ticket procedures, NMCI protocols, and act as intermediary for unresolved Trouble Tickets that exceed the SLA. Assist in determining whether an issue should be directed to the NMCI Help Desk or ONR OneDesk.
- Report all malfunctioning printers ports or drops to the CTR and NMCI.
- Prepare Move Add Change (MAC) requests.
- Research and prepare purchase request for items/services.
- Create, submit and monitor build-outs for services.

Requirements Management

- Conduct follow-up processes on all unresolved issues and escalate in accordance with the NMCI chain of command.
- Drafting service orders for Government approval, mapping applications, creating and submitting build-outs, reviewing and recommending approval of invoices, and updating template in ISF tools.
- Monitor all enterprise wide software updates to insure that the users receive updated software.
- Maintain and access the EITSMS.

Systems Management

- Monitor information on Homeport.
- Monitor NMCI alerts.
- Participate on development of business rules, processes and policies.
- Prepare agendas, supporting documentations, meeting notes, reports or presentations.
- Collect and analyze data as well as produce reports based on the data collected.
- Schedule all NIPRNET and SIPRNET services for ONR headquarters and field sites and schedule all upgrades, changes and alterations to current seats during Tech Refresh.
- Review/approve pre-invoices and invoices in eMp for all orders for headquarters and field sites.
- Maintain all necessary electronic and hard copy documentation.
- Maintain and track inventory at all ONR sites via the EITSMS Systems or similar.
- Maintain Command Application and Templates.

- Add and remove certified/decertified applications.
- Prepare documentation to create Request For Service numbers (RFS) for Command Application lists.

Account Management

Manage all user accounts to include the following:

- Activate or reactivate disabled accounts. Coordinate approvals with appropriate NMCI authorities.
- Create all new user accounts.
- Marry all permissions to ONR, and transfer all existing accounts to ONR as necessary.
- Assist new users in completion of UAIF forms and coordinate with NMCI.
- Deactivate user accounts.
- Transfer user accounts as necessary.
- Coordinate services with ONR OneDesk to ensure account creations, asset assignments, and other services are provided in a timely fashion.

3.2.2.3 HQ User Training

The Contractor shall create and manage a customer-training program to support the various ONR missions and objectives. The Contractor shall provide direct training, lecture or instruction, professional/technical development, in addition to the coordination and planning necessary to obtain services. However, the primary method of instruction shall be off-the-shelf or customized computer-based training packages under this CLIN to meet specific management and organizational needs. The frequency of training is primarily tied to the implementation of new capabilities for ONR.

The Contractor shall:

- Train ONR personnel on Command Standard software applications and designated information systems (IS). (See Section J, Attachment A-1 for a list of legacy software applications and designated IS).
- Develop IS and software application training courses and materials for these courses and (upon Government approval of training content) conduct the training. Update training materials to accommodate changes in the curriculum, applications, or information systems; and maintain an On-Line Library of training course materials.
- Conduct new or revised courses for trial groups of ONR personnel.
- Coordinate monthly training schedules with the client.
- Perform training classes on the use of IS resources (such as hardware, software, and security) and provide training certification to network administrators.

- In support of the ONR IAM, develop, design, and measure the effectiveness of information security training and awareness material provided to new hires, employees, reservists, contractors, and others who may have access to sensitive information or information systems.

3.2.3 Configuration and Enterprise License Management

The Contractor shall operate the current Configuration Management program on ONR networks to ensure applications do not cause conflicts and degrade network/operator performance. The Contractor shall document and track licenses and quantities for applications and software. The Contractor shall support hardware and software re-capitalization planning and manage the command approved software and hardware lists and associated documentation libraries. The Contractor shall provide technical inputs to policies and procedures; develop configuration management utilities; and recommend the use, operation, and maintenance of software and applications to support configuration management, asset management, and license management for all applications and systems. Patch and fix management is critical to preventing security breaches. The Contractor shall ensure all ONR systems, networked and stand-alone, thin or thick clients are properly secure with the latest software and firmware patches.

The Contractor shall operate a software inventory management program of legacy software to ensure compliance with DoD policy and other federal laws and commercial best practices. The Contractor shall monitor, track, and ensure that the software in use on all ONR networks have licenses and notify ONR IT managers when maintenance agreements are to expire. Any licenses or hardware purchased by the contractor shall be titled to ONR. The Contractor shall research licensing alternatives and present the best licensing alternatives to ONR. The Contractor shall consider usage trends, migration plans, operational changes, and return on investment (ROI) when researching alternatives. The Contractor's program shall maximize ROI and maintain the warranty and maintenance coverage for all hardware and software (including contractor purchased items and Government purchased items).

The Contractor shall maintain and control all versions of existing Configuration Items (CIs) used in the provision and management of its IT services at ONR. The Contractor shall perform and provide configuration management that is accurate and up-to-date by managing the life cycle of all CIs from acquisition to termination.

The Contractor shall track user requirements and work with the numerous governance boards to collaborate and manage changes in requirements, business processes, software, and IT policy.

The Contractor shall:

- Implement a hardware and software maintenance/warranty program to monitor and track assets.
- Analyze and support ONR management on the development of configuration management policies and procedures for CIO approval and implementation.
- Ensure DoD and DON patch mandates (IAVM compliance) are met within specified time requirements.
- Comply with the mandatory information security standards/configurations specified in the applicable Department of Defense (DoD) Security Technical Implementation Guides (STIGs).
- Implement automated systems for patch management.
- Implement Government approved configuration management modules.
- Develop configuration management utilities to automate software and applications for configuration management, asset management, and license management.
- Update configuration-management policy documents upon CIO concurrence.
- Maintain the command approved hardware/software list.
- Record and publish minutes of the Configuration Management Board (CMB), the Infrastructure Configuration Control Board (ICCB), and the Applications Configuration Control Board (ACCB).
- Track licenses, maintenance plan and warranty information for all software and hardware on the ONR networks.
- Coordinate with appropriate ONR staff when users request upgrades to existing legacy applications, and maintain configuration documentation.
- Implement a Configuration Management Database (CMDB) that contains details of the CIs throughout their life cycle and that provides accurate information to support all the other service management processes.
- Establish and maintain the Definitive Software Library (DSL) and Definitive Hardware Library (DHL) stored in the CMDB.
- Maintain the library of Standard Operation Procedures (SOPs) and ensure that the SOPs are accurate and reflect current, approved practices.
- Conduct reviews that assert that CIs actually exist, and check that these CIs are correctly detailed in the CMDB.
- Provide recommendations for changes to the CIs to include suggestions for new procedures, additional skill sets, technology refreshment, and modified configurations.
- Develop and implement a plan to replace key IT assets and CIs at regular intervals throughout their life-cycle.

- Receive, store, distribute and dispose of assets and CIs.

3.2.4 Acquire IT Assets

The Contractor shall use Government-approved procurement procedures to acquire (upon Government approval) IT assets, e.g., equipment, software, communications, and services in support of this contract.

The Contractor shall:

- Procure, with Government approval, software, hardware, upgrades, licenses, maintenance agreements, and spare parts. The Contractor shall ensure that all hardware provided has the most cost-effective warranty available from the vendor. In most cases, warranty coverage should be for parts only versus on-site warranty coverage.
- Follow Government guidance and categorize all procurements as either: (1) Mission Critical, (2) Urgent, or (3) Routine. Deliveries shall be timely, in accordance with the prioritization of the requirement. All acquired Information Technology assets (i.e. Software, Hardware, Documentation, etc.) shall immediately become property of the Government.
- Comply with the DoD CIO Guidance and Policy Memorandum No. 12-8430-July 26, 2000 – Acquiring Commercially Available Software, for all software acquired by the Contractor for this contract. Detailed information can be found on the Enterprise Software Initiative Home Page: http://www.don-imit.navy.mil/esi.
- Provide Asset Management support to ONR to ensure that all information systems hardware and software are properly received, documented, stored, and disbursed to the required user to maintain good supply and accountability of Automatic Data Processing Equipment (ADPE).
- Coordinate the disposal of property, supplies, and or material in compliance with government and /or military regulations /guidelines.
- Maintain an up-to-date inventory of all current hardware and software, including spare items (by item description and serial number) as well as original software diskettes, CD-ROMS, DVDs, URL download information, manuals, and books. Notify the government as spare items become depleted to allow for replenishment. Attachment A-2 (ONR Physical Inventory) contains an inventory of the current hardware, software, and maintenance contracts.
- Follow the DON CIO Information Assurance Strategy Guidance Template found at http://www.doncio.navy.mil/ContentView.aspx?ID=676

3.3 TASK AREA 3 - STRATEGIC ARCHITECTURES AND PROGRAM SUPPORT

3.3.1 Program Support

3.3.1.1 Emerging Business Technology Support

The Contractor shall provide support to implement a program that properly integrates new systems into ONR as well as a plan to support the transition out of legacy systems (See Attachment A-1) as appropriate. ONR also needs to have more visibility into Life Cycle Management issues for maintaining existing systems and fielding new IT systems. By spending more time coordinating, planning and integrating IT systems in the procurement process, the Government will be able to focus on matching requirements (capability) with resources (finances) for the short-term and create a more cohesive long-term plan to serve the Command.

ONR specifically requires systems engineering and technical integration support for technology insertions in support of the ONR mission.

The Contractor shall:

- Provide technical integration tasks to include testing and evaluating system architectures/engineering designs.
- Recommend technical solutions to system shortfalls, emerging technologies or proposed projects.
- Perform technical system configuration and administration in accordance with industry best practices, system documentation, and the Program Management Plan.
- Develop training materials and deliver administrator training.
- Maintain technical systems documentation, test results, and administrator training materials.
- Test and evaluate system architectures and engineering designs.
- Analyze integration efforts to ensure compatibility and functional performance compliance to the requirements in consideration of future projects or upgrades. Identify projected shortfalls and recommend corresponding solutions.
- Develop and execute operational tests to the systems to assure compatibility and functional performance.
- Perform business process analysis, define requirements, and produce program documentation.
- Develop a comprehensive transition plan for the program.

- Develop comprehensive strategic engagement plans to shape Service and DoD level programs in support of ONR's mission requirements.
- Draft ONR Policy and Guidance to govern the use of program area applications, systems, and IT capabilities.
- Research and develop initial Project Management Charters (PMC), kick-off briefings, and Project Scope Statements.
- Produce decision and information briefings/papers and status frameworks for all applicable programs, projects or processes.
- Develop Project Plans for technology insertion projects.
- Develop project-level resource and procurement strategies via a financial plan to execute technology insertion projects.
- Develop Management Structures to ensure all manpower and support relationships are well-defined to support implementation and transition to operations and maintenance.
- Perform detailed systems analysis and design for development of Operational/Functional, Systems, and Technical Architectures.
- Develop, coordinate, or review detailed Certification and Accreditation documentation in accordance with DoD Instruction 8510.01 - DoD Information Assurance Certification and Accreditation Process (DIACAP).
- Analyze risks, and develop accompanying mitigation plans to support ONR-wide technology insertions.
- Develop Quality Assurance and Testing Plans to ensure interoperability with current ONR Command, Control, Communications, and Computers (C4) baseline.
- Develop integrated program control processes and robust network operational frameworks for all technology insertions prior to transition to operations and maintenance activities.
- In coordination with Operations, transition technology insertion to full operational capability with defined change control processes properly articulated in applicable ONR regulations.
- Produce decision and information briefings/papers and status frameworks for all applicable projects or processes.
- Document Lessons Learned in accordance with CIO Lessons Learned policies and procedures.
- Follow the DON CIO Information Assurance Strategy Guidance Template found at http://www.doncio.navy.mil/ContentView.aspx?ID=676

3.3.1.2 Command Information Officer (CIO) Support

The CIO is the primary interpreter of operational technology issues and decisions within ONR. The CIO office is responsible for monitoring, assessing, and evaluating technology; recommending appropriate technology solutions to support polices and directives issued by ONR and mandated by government; and supporting ONR strategic plans and initiatives.

The Contractor shall:

- Provide data for and support the development of white papers, information papers, point papers, PowerPoint presentations, spreadsheets, databases, policy, and guidance, etc. in accordance with ONR regulations, standards, and processes to facilitate and aid in the development of CIO objectives and goals in support of the ONR Strategic Plan.
- Identify gaps in Information Resource Management (IRM) strategy and policies.
- Research and propose solutions to enable the modernization of the ONR IT architecture and the integration with new technologies. Monitor emerging technologies and industry best practices and provide recommendation for IT refresh opportunities.
- As required/directed, attend approximately 10 working groups, meetings, and conferences annually (stateside and overseas).
- Advise the CIO regarding a Net-Centric enterprise approach to Information Resource Management (IRM) and IT application within the command and provide input into the strategic planning process.
- Lead, develop and evaluate technology support, infrastructure operations, COTS/GOTS systems, custom applications, governing policies, Information Assurance and standards needed to provide flexible and effective IT services and capabilities.
- Ensure that the ONR strategic plan is supported by the latest in proven advanced technology by monitoring, assessing and evaluating emerging technological solutions.
- Gather technology requirements from CIO for evaluation, acquisition recommendation, and implementation.

3.3.2 Strategic C4 and Architectures Support

The Contractor shall be the ONR Enterprise Architecture (EA) developer. This includes researching EA products, developing federated EA products and providing solutions to ONR EA issues. The ONR EA will align to the DoD EA and the DoD Joint Capability Areas (JCA). The Contractor shall comply with and incorporate existing and future ONR planning documents as well as apply Government and industry best standards to

include compliance with the DoD Architecture Framework (DODAF), modified to reflect the ONR environment. Policy guidance such as the DON Memorandum Department of Navy Enterprise Architecture Strategy dated 18 February 2009 and Implementation and use of Department of the Navy (DON) Enterprise Architecture (EA) Hierarchy dated 06 January 2009 are located on the DON CIO Website at http://doncio.navy.mil/policy.aspx.

The Contractor shall:

- Understand Command strategies, missions, roles, functions, and ONR support requirements. Conduct near-, mid-, and long-term enterprise and strategic C4 planning.
- Research, develop, and maintain the Command Enterprise Architecture including architecture products for operational, system, and technical components.
- Research, design, and develop technical specification for ONR's information systems and their interfaces with other DoD and non-DoD systems.
- Assure Contractor team produces domain architectures which fully address mission threads (operational facilities, tasks, billets, and processes) and current and future C2, Net-Centric capabilities.
- Analyze ONR architectures, Business, and Enterprise Information Environment (EIE) processes, and IT to identify mission capability gaps, overlaps, and shortfalls and recommend architectural, IT, or process solutions.
- Research and develop other EA component and architecture documents and plans.
- Understand and use the DOD Architecture Framework and other key DoD architecture and net-centric planning instructions.
- Collect data and conduct ONR EA strategic planning.
- Identify future technology capabilities and potential architectural and capability impacts for ONR.
- Conduct architecture tool analysis and recommend tools for ONR use based on approved DoD and industry best standards.
- Understand architecture tool capabilities and functioning and employ tools such as the Joint Command and Control (JC2) Architecture Capabilities Assessment Environment (JACAE), MS Professional, ProVision, and Telelogic System Architect.
- Understand and use the DoD Architecture Repository System (DARS). Participate in DON Enterprise Architecture Conferences, Communications Conferences, and Architecture Working Groups.
- Attend DON meetings.
- Develop and maintain effective working relationships with the ONR Staff and counterparts at OASN (RD&A).

- Develop and support an ONR Data Architecture.
- Participate with the ONR Working Group in the development of a Continuity of Operations Plan (COOP).
- Develop and maintain architectural drawings for all ONR systems as required.

3.4 TASK AREA 4 - LEGACY NETWORK INFORMATION ASSURANCE (IA)/COMPUTER NETWORK DEFENSE (CND)

3.4.1 Information Assurance/Computer Network Defense

The Contractor shall provide security management support for Information Assurance (IA) and Computer Network Defense (CND). The objective of this task is to support ONR's efforts to direct and synchronize IA-CND actions and activities to proactively defend the ONR portion of the Global Information Grid (GIG) and to provide ONR network security situational awareness to the Chief of Naval Research (CNR).

3.4.2 ONR Network Security Support

The Contractor shall provide IA and CND support for ONR Security Policy, plans, exercise, DISN connection Approval, Cross Domain Solutions and security engineering. The Contractor shall provide a complete and thorough picture of the ONR Information Assurance Common Operating Picture (IA COP) through analysis and correlation of events.

The Contractor shall:

- Provide ONR IA and CND situational awareness.
- Maintain oversight of ONR ports and protocols program.
- Enforce accreditation, certification and connection standards for ONR networks and systems.
- Establish, maintain and enforce IA and CND policy.
- Protect and defend the ONR IT Infrastructure.

The Contractor shall provide support for the following specific task areas:

3.4.3 Network Security Operations Engineering

The Contractor shall:

- Supervise and conduct crisis action planning and security engineering.
- Coordinate integration of IA-CND activities with other Network Operations Functional Areas, with Information Operations, and operational requirements.

- Provide support for IA-CND Network Operations Functional Area Lead responsibilities.
- Review network architectures to ensure they meet DOD/ONR security configuration requirements and regulations.
- Analyze and manage the ONR Enterprise Sensor Grid.
- Provide data for Navy On-Line Compliance Reporting System (OCRS) account management and support.
- Review, support, and when directed perform ONR assessments and provide recommendations on targeting, mitigation actions, priorities, and technical solutions.
- Provide ONR CIO staff with security engineering design support during the planning, execution, and after-action phases of exercises, contingency operations, and current daily operations.
- Perform network security engineering, planning/design, analysis, and technical monitoring of tasks.
- Perform network review/validation of network topology and architecture plans, review/validation of configuration changes, and review and risk assessment of new and/or upgraded technologies.
- Provide technical assistance with the design, installation, operation, service and maintenance of a variety of multi-user information security systems such as virtual private networks (VPNs).
- Configure and set up information security systems such as firewalls.
- Provide technical assistance with the initial set-up and secure deployment of systems that support information security including virus detection systems, firewall content filtering systems, web site blocking systems, intrusion detection systems, intrusion prevention systems, software license management systems, single sign-on systems, centralized multi-platform access control databases, and enterprise security management systems.
- Manage ONR's ports and protocols program, including the processing and tracking of firewall exception requests.
- Review, scan, and configure new, upgraded, and existing systems to ensure security compliance IAW policy directives and DISA Security Technical Implementation Guides (STIGs) are completed.
- Collect, review, maintain, and analyze sensor data to identify performance and anomaly issues.
- Review/analyze vulnerability scanning data and intelligence information to provide recommendations and/or direction to mitigate vulnerabilities and threats and to validate corrections.
- Develop ONR technical standards for security devices, security operations and other operations as required. Write associated Standard Operating Procedures (SOPs)/ Tactics, Techniques, and Procedures (TTPs), technical implementation instructions, or other required documentation.
- Conduct information collection and dissemination through use of IA-CND intelligence products, databases, websites, and tools; military and commercial/open source products, databases, websites, and tools; locally

generated databases, websites, and tools; and any other relevant source of information and intelligence, to include:

  - NNWC (NNWC) Cyber Alerts
  - Navy Computer Tasking Orders (CTO)
  - Combatant Command (COCOM) / Service / Agency (CC/S/A) information websites, databases and products
  - Correlation Tool queries
  - Host Based Security System (HBSS) reports/queries
  - User Defined Operational Picture (UDOP) (when it becomes available to ONR) monitoring of national and ONR IA-CND information
  - Traffic Network Management Agent (TNMA) related tools for IA-CND specific information queries and analysis
  - Commercial sources and systems
  - Audit logs, System Logs, and other data
  - Network scan results
  - Other sources and tools as required.

- Review and validate implementation of policies and standards through HBSS and SmartFISMA.
- Develop metrics dashboards to ensure the goals and objectives of FISMA are identified and met annually and IAVA compliance can be measured.
- Conduct security metrics measurements to support analysis and improvement of ONR IA-CND performance/capability metrics.
- Coordinate with the ONR enterprise engineering personnel to provide security expertise, support planning and identify issues and mitigation.
- Assist ONR in IA-CND operational and planning efforts.
- Lead/conduct collaboration for IA-CND planning and operations, e.g., email, chat, ticketing and collaboration session communications.
- Support Naval Network Warfare Command (NNWC) and DON CIO Conferences, Exercises, and Policy guidance.
- Serve as an Action Officer; Operational Planning Team Member; or lead/supporting member for operational and/or planning tasks assigned to IA-CND as required; respond to Naval Network Warfare Command (NNWC), Defense Research and Engineering Network (DREN), and DON taskers and RFIs as required (with Government approval).
- Implement Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan IAW DODI 8510.01
- Develop DIACAP documentation as required.
- Conduct DIACAP Validation Activities - Validation includes all tasks related to the execution of validation procedures (VPs) that are associated with assigned IA controls. Each VP describes requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocol for recording actual results. VPs may include associated supporting background material, sample results, or links to automated testing tools.

3.4.4 Accreditations and Connection Approval Engineering

The Contractor shall provide the following accreditations and connection approval engineering support:

- Provide data to support the execution of the Chief of Naval Research's (CNR) Echelon I and II Certification & Accreditation Program as defined by the Navy Office of Designation Approval Authority/Certification Authority (ODAA/CA) and the High Performance Computing (HPC) Modernization Program Office (HPCMPO).
- Ensure current networks and systems maintain certification and authority to operate as they are modified to meet operational requirements.
- Track and maintain certification information databases, websites and tools to ensure that ONR networks, systems and devices are properly documented and managed from a security perspective. These include:
    - SNAP (Standard Network Access Protocol) database
    - Local databases, sites and systems
    - Information Assurance Tracking System (IATS)
- Coordinate with subordinate, adjacent, supporting and senior organizations and agencies to support resolution of security issues, accreditation and connection approval, and waiver requests.
- Recommend connection approval, disapproval or modification based on security risks and vulnerability.
- Recommend network configuration, policy, training, operational or other changes/updates based on assessed risks and/or issues.
- Advise the ONR IAM and the Designated Approval Authority (DAA) of network and system risks, risk mitigation courses of action and operational recommendations.
- Review new and existing systems and devices for security risks and certification/accreditation in support of technical approval by ONR CIO in coordination with the ONR CIO office, and other ONR staff organizations.
- Provide security-engineering review for ONR system/network initiatives
- Review Security Test and Evaluation plans; develop as required.
- Perform network security accreditation and policy support tasks, including project management support services.
- Perform review, analysis, and documentation for the life-cycle security requirements of applications, systems, and networks within the ONR IT Infrastructure. Utilize Common Criteria, Secret and Below Interoperability (SABI), DoD security accreditation and DISA network connection approval security processes for computer systems or networks. Support security design, testing, and implementation requirements of integrated networks to include hardware, software and port protocols and services.
- Lead/conduct ONR collaboration for IA-CND planning and operations.
- Support Naval Network Warfare Command (NNWC) and DON CIO Conferences, Exercises, and Policy guidance.

- Serve as an Action Officer; Operational Planning Team Member; or lead/supporting member for operational and/or planning tasks assigned to the IA Branch as required; respond to NNWC and DON taskers and RFIs as required (with Government approval).
- Conduct any other tasks relevant to duty description or deemed necessary by the government to achieve mission success.
- Perform certification and accreditation for ONR systems and networks fielded or supported by ONR CIO staff IAW DIACAP requirements.
- Review and support certification and accreditation for ONR systems and networks fielded or supported by ONR staff directorates and other offices.
- Complete security documentation and security analysis for major applications, hardware and support systems IAW DIACAP standards.
- Serve as IA point of contact for promotional, test, new, replacement and/or Contractor equipment brought into the purview of the ONR type accreditation. Once equipment is identified, ensure the owners of the equipment provide proper accreditation documentation and make necessary changes/additions to the DIACAP Implementation Plan (DIP).
- Perform Automated Information Systems (AIS) security inspections periodically for CIO managed systems, no less than annually, in order to ensure the accuracy of the DIP. Make changes and updates.
- Provide C&A accreditation/AIS security support.

3.4.5 Headquarters Information Assurance & Network Defense

The Contractor shall protect the ONR Infrastructure, to include HQ, ONR Global and other field activities under CNR control. The Information Assurance / Computer Network Defense (IA/CND) program will support Command Security Policy, plans, exercises, Certification and Accreditation, and Incident Handling and Response.

All Information Assurance (IA) will be in compliance with the following:

- SECNAV M-5239.1 DON Information Assurance Program; Information Assurance Manual
- National Industrial Security Program Operating Manual (NISPOM)
- CJCSI 6211.02 (series)-- Defense Information System Network (DISN): Policy Responsibilities and Processes of 31 July 2003
- CJCSI 6212.01 (series) -- Interoperability and Supportability of Information Technology and National Security Systems
- DOD 5200.2-R – Personnel Security Program
- DoDD 8100.1 -- Global Information Grid (GIG) Overarching Policy
- DoDD 8500.1-- Information Assurance
- DoDI 8500.2 -- Information Assurance Implementation

- DoDI M-8510.1 -- DoD Information Assurance Certification and Accreditation Process (DIACAP) Application Manual
- DoDI 8570.1 -- Information Assurance Training, Certification, and Workforce Management
- SECNAV M-5239.2 DON Information Assurance Workforce Management Manual
- SECNAVINT 5239.3B DON Information Assurance
- CNO N614/HQMC C4--Navy Marine Corps Unclassified Trusted Network Protection (UTN-Protect) Policy, Version 1.0, 31 October 2002

The Contractor shall:

- Analyze and isolate security intrusions, security incidents/compromises and viruses of HQ servers and clients and on request, assist ONRG with such efforts.
- Report incidents to the IAO, IAM, CIO, and senior leadership.
- Provide and maintain an effective security awareness and training program in accordance with Federal and DoD policies and standards.
- Review and provide input to NNWC, DREN and DON Taskers (with Government approval).
- Review all HQs and ONR Global (if in ONR HQ resource forest) server audit logs for analysis and determination of actual or attempted security breaches.
- Analyze security events triggered on HQ and ONR Global routers, firewalls and IPS sensors.
- Provide Trend analysis of events, ensuring best security practices and identifying misrouted traffic.
- Support HQs security traffic analysis; network optimization program.
- With coordination with the IAO, maintain or develop new accreditation of all HQs systems and networks IAW DIACAP.
- Integrate with the Change Management process, ensuring new systems meet existing security requirements or policy.
- Perform IAVM Compliance Validation and Reporting.
- Conduct Network and System Security reviews (reportable under FISMA); to include vulnerability scanning of HQ networks.
- Conduct vulnerability assessments on new hardware/software.
- Maintain configuration of all ONR Net Defense tools (i.e., firewalls, IPS, ADS, HIDS, XACTA, eTrust, Securify, etc.).
- Lead and coordinate Navy Echelon I/II C&A efforts that shall certify and accredit Information Systems through an enterprise process for identifying, implementing, and managing IA capabilities and services. IA capabilities and services are expressed as IA controls as defined in DODI 8500.2. IA controls are maintained through a DoD-wide configuration control and management (CCM) process that considers the Global Information Grid (GIG) architecture and risk assessments that are conducted at DoD-wide, mission area (MA), DoD Component, and IS

levels consistent with Subchapter III of Chapter 35 of title 44, United States Code, "Federal Information Security Management Act (FISMA) of 2002"

3.5 TASK AREA 5 - BUSINESS AND RESOURCE MANAGEMENT SUPPORT

3.5.1 Information Technology Infrastructure Library (ITIL)

ONR requires support to implement a program that enables ONR to successfully transition its IT organization to an ITIL operated environment. ITIL provides a number of important IT practices, comprehensive checklists, tasks and procedures tailored to manage IT services and operations. The contractor shall deliver a comprehensive plan for ITIL implementation within 90 days of contract award.

3.5.2 Business Intelligence (BI)

ONR currently uses the Oracle Analytics tool to support its BI environment. The contractor shall provide services to coordinate planning and transition activities across projects between the Command Business Office and the Chief Information Office. The contractor shall ensure that reliable and secure information and data is available in the BI environment and reported to key stakeholders and decision makers in a timely manner to prevent disruption in day to day IT services and unnecessary delays in project deliverables.

3.5.3 Enterprise Resource Planning (ERP)

ONR requires support to enable ONR Headquarters, CONUS Field Offices and Global Offices to successfully transition to the Navy Enterprise Resource Planning (ERP) system. In order for ONR to receive the maximum benefit, the program must incorporate Navy ERP, NMCI, ONR's current unique system requirements, the Navy's direction and business rules, SAP, and how the Navy has adopted SAP. To accomplish this task, ONR has begun the reengineering of current processes and procedures through Business Process Improvement (BPI). The contractor must work with the ONR and the current ERP contractors to help and support the transition to ERP. The Contractor must also have a solid, repeatable and well-established BPI methodology and approach in order to ensure ONR's success with this task.

The Contractor shall:

- Monitor the bandwidth being used to connect to the Navy ERP systems, identify and report when level reach saturation levels, and then recommend courses of corrective action.
- Monitor CITRIX systems to ensure that enough capability exists to connect with Navy ERP.
- Support mock ERP conversions as required and final cutover as required.

- Validate the documentation and mapping of legacy IT technology and associated software applications.
- Support legacy application shutdown planning to help the customers in knowing how to transfer the data to Navy ERP.
- Provide functional knowledge of Navy ERP so that questions can be answered, such as how to move data from one system to the next and how ONR employees can report business metrics from the new system as they did from the legacy system.
- Develop Navy ERP functional insight into ONR's Business Processes to assist with cut over activities.
- Work with Navy ERP and ONR staff to build a cutover plan for ONR that outlines such activities as the following: how the required data will be transferred from legacy systems (See Attachment O) or manual inputs; in what sequence (building in dependencies on data loads); using what validation routines; and when the events will occur.
- Understand the roles and assignments each person within ONR will be required to fill in order to continue to perform his duties after ERP implementation.
- Provide support for transition activities.
- Support team leads and subject matter experts (SMEs) with documenting transition plans.
- Assist with the coordination of transition activities.
- Assist with facilitating execution of approved transition plans.
- Build a strong working relationship and act as a liaison with the ONR ERP Help desk to enable timely responses to customers.
- Develop a strategy to protect corporate information that does not transition to ERP. The data should be available to ONR staff in a format that is readable and actionable.

3.5.4 Award Writing Tool (AWT)

The contactor will support the hosting of the Award Writing Tool (AWT) for approximately 130 users and associated maintenance support to upload system updates/version changes. When ONR transitions to Navy ERP, it is anticipated that Navy ERP will generate purchase request data, which will be passed to the AWT. The contractor shall be prepared for any data reformatting or other modification as required to interact with the AWT Application Program Interface (API). The contractor shall also ensure that the Extended Mark-up Language (XML) output from the AWT will conform to Navy ERP requirements.

3.5.5 Knowledge Management (KM)

The contractor shall provide services to coordinate planning and transition activities that promote and encourage the sharing of information and knowledge across projects between the Command Business Office, the Command Information Office, and ONR Headquarters and Global staffs. The contractor shall ensure that intellectual capital is valued as a corporate asset and aid in reducing redundant work and training time for new

employees. Contractor shall ensure that a KM environment is secure and available and optimizes the Total Cost of Ownership leading to increased efficiency in information, product delivery, and lessons learned.

3.6 TASK AREA 6 - APPLICATIONS AND WEB DEVELOPMENT

3.6.1 Software Development Support

The Contractor shall provide software development services to maintain ONR's mission critical applications. The contractor shall provide development and analysis support to maintain and improve existing capabilities and to perform general maintenance for bug fixes. The contractor shall maintain an automated track of software problems; applying proper analysis, process, and scheduling to repair deficiencies to avoid data integrity problems and useless system workarounds. (Section J Attachment A-1 includes a list and short description of current mission critical applications).

The Contractor shall provide support for a Business Intelligence (BI) component to the NAVRIS application using Oracle's Analytics BI software. BI component consists of interactive dashboards and charts with drill downs to detail and summary level reporting structures. Information is displayed on workload, work execution, and business performance. Contractor shall maintain a daily Extract, Transform, and Load (ETL) process to extract data from multiple sources and load into a data warehouse to maintain data quality and a single source of truth.

Contractor shall:

- Tailor Application designs and solutions to provide:
    - Improved business processes
    - Data integrity and stability
    - An enterprise wide common framework
    - Increased employee productivity and collaboration
    - Reduced data redundancy.
    - Streamlined infrastructure
    - Overall reduction in costs of doing business
    - Appropriate documentation on any environmental modifications that will impact accessibility and availability of applications and data prior to modifications
    - Business Activity that is stable, secure, and reliable

- Provide project tracking and oversight for adequate visibility into progress, so management can take corrective action if work performance deviates significantly from the plan. Tracking and oversight involve reviewing work accomplishments against documented estimates, commitments, measures and metrics, plans, and schedules; and taking corrective action when the plans are not being met.

- Use a structured methodology to promote agility and repeatability in the development process. Process shall be adaptive to customer involvement throughout an iterative development process.
- Propose a software development methodology that will support the guidelines of this performance work statement for approval by the ONR TPOC within 30 days of Contract award. The current ONR software development process is being managed in accordance with an ONR Software Development Plan (SDP) dated June 2004 (a modified version of SEI CMM Level 2), and it defines the organizational structure, policies, and processes used and can be used as a baseline to build from. Additionally, ONR has chosen ITIL for its service delivery and management, and any software methodology proposed must be consistent with the ITIL framework. Once the new Software Develop Plan is approved by the TPOC, the contractor shall follow the plan and monitor processes to ensure that all important steps in the development process have been adequately performed.
- Maintain a development framework that includes all phases of the development life cycle including Project Management, scope and initiation, requirement gathering, design, development, product test and assessment, deployment, training, and closeout. Also included are communications, configuration management, quality assurance, IA compliance, and collaboration. Contractor shall also manage any improvements to the software after deployment and diligently and clearly document all customized software, including data base triggers / packages and workflows, to facilitate future maintenance and enhancements.
- Ensure compliance with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards Act implemented at 36 CFR Part 1194.
- Perform Systems Analysis by gathering high-level functional requirements, documenting results and findings, and recommending course of action.
- Provide System Development Life Cycle support for fielded software baselines as well as for commercial-of-the-shelf (COTS) and Government-of-the-shelf (GOTS) software.
- Ensure the technology products, services, and solutions provided are of high quality and fully integrated and tested to include hardware, software, security, operating systems, and networks.
- Use the mature development process in all software development and maintenance activities. Mature software development processes are documented, predicable, repeatable, and manageable in terms of quality, cost, schedule, and performance.
- Help the In-House Training team develop user-training materials to assist users in properly using the business applications software.

- Perform Oracle DataBase and System Administration support for all Oracle based applications residing on the ONR legacy network. The contractor shall maintain and administer all Oracle Production, Development, Data Warehouse, Testing, and Training instances and their environments. Data Base environments must be available 24 hours a day, 7 days a week, except during general maintenance and data base backups. The contractor is responsible for assuring that the COR and ONR TPOC are kept aware of any database and system related incidents resorting in down time, inefficient processing, data base integrity, etc. The contractor shall provide:
    - Schema, space, and performance management
    - Data base refreshes and exports
    - Data base backup and recovery services
    - Data base installs, upgrades, and patches
    - Capacity planning; data base security; and data base instance management
    - Administration and maintenance of all the Electronic Data Interchange Production and Development Servers and their environments
    - System availability 24 hours a day and 7 days a week with a 98% availability rating (excluding normal downtime for system maintenance and backups)
    - A system with satisfactory performance without latency issues
    - Effective management of software patches and upgrades associated with the Oracle e-Business Application software, Oracle data bases, and LINUX operating system software that maintains the reliability and quality of ONR's application infrastructure
    - Assurance that adequate disaster recovery assets exist for critical systems to recover from data corruption and catastrophic hardware failure scenarios
    - Day-to-day management and operations assignment and distribution of database users accounts and initial expired passwords to authorized users.
    - System Administration services
    - User access control privileges at the data base level in response to ONR management instructions and communicating any delay in posting requested change.
    - Adherence to information security policies, guidelines, procedures, and other requirements when assigning and updating the privileges of users in shared databases.
    - Processes that securely preserve all records indicating changes to access control privileges to facilitate investigations, disciplinary actions and prosecutions.
    - Reports that generate analysis data indicating database activity to highlight potential performance problems, security violations, and other problems needing attention.

- Develop and maintain strategies of communications, configuration management, quality assurance, IA compliance, and collaboration.
- Ensure applicable STIG configurations are in place.
- Ensure that new fieldings follow the DON CIO Information Assurance Strategy Guidance Template found at http://www.doncio.navy.mil/ContentView.aspx?ID=676
- Develop and maintain a repository for enterprise level business rules, system data flow diagrams, and requirements to facilitate system design integrity and ensure higher productivity, reduced errors, and tighter compliance with regulatory/policy requirements.
- Provide technical assistance for the C4 systems requirements process within ONR.
- Maintain proper version and configuration management control of all software applications. ONR currently uses Serena Corporation's Professional Version Control Software (PVCS) to manage software versioning and control.
- Provide for the management of and access to data from ONR's core mission critical applications, such as NAVRIS, AwardWeb, eProposal, Business Intelligence, and IPMIS after the transition to Navy ERP.
- Provide support to ONR functional codes for their organizational IT support contractors that manage and maintain software applications specific to their unique business processes. Applications may reside on the ONR Legacy network or in the NMCI hosting facility. Support requirements shall include server hosting and management, operating system maintenance, and general network operational functions such as backup and recovery.
- Implement DIACAP Implementation Plan IAW DODI 8510.01.
- With coordination with the IAO, maintain or develop new accreditation of all systems under this purview IAW DIACAP.
- Conduct DIACAP Validation Activities - Validation includes all tasks related to the execution of validation procedures (VPs) that are associated with assigned IA controls. Each VP describes requisite preparatory steps and conditions, actual validation steps, expected results, and criteria and protocol for recording actual results. VPs may include associated supporting background material, sample results, or links to automated testing tools.

3.6.2 Web and Structured Query Language (SQL) Server Database Support

Contractor is required to develop, network, and integrate command web systems and databases, which provide support of day-to-day ONR headquarters and Field Office operations. The Contractor shall provide direct technical support, testing, systems integration, application development, and maintenance in support of ONR C4 initiatives for the SIPRNET, DREN and NIPRNET networks. This environment will continue to

evolve from the current state toward a portal environment. This portal environment shall be role based and shall provide the user with a view of enterprise information, knowledge, and applications based on their role in the organization, with single sign-on access capabilities. This task will support all migration efforts of the intranet, extranet, and internet environments.

The Contractor shall:

- Provide technical support based on Web policies stated in OSD Web Site Administration, DoD Instruction 5230.29, DoD Directive 5230.9, DoD Directive 5200.40, DoD Instruction 8510.01 and SECNAVINST 5720.47B.
- Provide systems integration, testing, maintenance, installation, configuration, and troubleshooting for all databases and web applications.
- Serve as technical database systems administrator for the Command's SQL databases and multiple SQL servers; and serve as technical expert on all web servers.
- Monitor operation of databases/web servers to ensure that software and hardware are functioning properly for secure, reliable, and stable operations.
- Generate and distribute outbound Internet web browsing activity reports, including attempted but denied connections for IAO and ONR IAM review and remedial action.
- Periodically review access control logs and reports to ensure that the web sites are working properly and that no unauthorized activity is taking place.
- Provide technical guidance on the implementation of new web, database, and portal software.
- Implement security and access controls requested by content providers and page maintainers as required.
- Install, maintain, and operate filtering software that screens inbound information flows for viruses, Trojan horses, and other unauthorized software, and screens outbound web traffic such that this traffic only connects to sites that are consistent with authorized business purposes.
- Install, maintain, and operate change detection software that immediately flags any changes to critical software or files on Internet connected systems.
- Install and fine tune load balancing software that allocates traffic to various machines on the web/electronic commerce systems.
- Participate on a Computer Incident Response team that responds to various Internet –based security incidents such as denial of service attacks and infestations.
- Immediately remove all unauthorized content or programs that have been place on the web/electronic commerce site to limit ONR liability and to thwart intruders.

- Establish and monitor automated time synchronization systems so that all web/electronic commerce system logs reflect accurate time/date stamps.
- Work with ONR Subject Matter Experts (SMEs) to capture and document business processes through customer interviews and requirements gathering.
- Develop software design documents (SDD) for creation of Knowledge Management functions within the Portal environment.
- Ensure system integration, architecture, data integrity, and integration efforts conform to DoD standards.
- Manage the gathering, documenting, testing, deploying, and marketing of web content to support business processes within ONR.
- Support Web/database development and administration on the SIPRNET, NIPRNET. The Contractor shall be responsible for all SQL databases and web applications/pages.
- Convert and develop SQL databases to support Command's requirements.
- Develop, test, and implement web parts for the Portal.
- Provide advice and development support for the introduction of capabilities such as blogging, wikis, tagging, online collaboration, and social networking with the power to create, shape, and customize user information, application, and work experience around tasks that users need to accomplish sharing ideas and information with other ONR users.
- Draft policy and procedures for training users on new web/database applications.
- Troubleshoot issues with existing or developed systems, and work with the appropriate resources to resolve them.
- Write code for development efforts using C, SQL, ASP .NET, VB and JAVA scripts.
- Write Stored Procedures and Triggers to incorporate them into the database development.
- Develop, maintain and administer command level web pages on the ONR INTRANET, SIPRNET, and NIPRNET.
- Identify, recommend, develop, and implement web tools and applications.
- Coordinate/assist directorate/agency webmasters in developing web/portal pages.
- Integrate directorate/agency web/portal pages with command level pages.
- Develop web interfaces to command and directorate/agency databases and files. Identify, recommend, develop and implement solutions to customer requirements for greater availability to data and services hosted on the web.
- Operate, maintain, and administer 2 web and SQL servers, hardware and software.

- Coordinate with network system administrators to minimize network service disruption.
- Comply with the mandatory information security standards/configurations specified in the applicable Department of Defense (DoD) Security Technical Implementation Guides (STIGs).
- Develop and document web management and user guidance on use and management of web pages and provide input to web policy guidance for the command.
- Provide ongoing support, resolution of problems, and recovery of operational malfunctions involving hardware/software failure.
- Coordinate with Security personnel to ensure that the latest Information Assurance Vulnerability Management Alerts/Bulletins (IAVMs) are loaded within the designated timeframe. Evaluate and determine whether vendor-supplied system patches and fixes will cause software incompatibility trouble, system crashes, systems response time degradation, and/or other operational problems before installing patches and fixes.
- Identify and assign (with Government approval) permissions and roles to databases.
- Analyze database design and structure; and recommend changes to improve performance.
- Provide training to functional area database administrators.
- Document all upgrades to hardware and software.
- Utilize Configuration Management practices.
- Keep database server information current in database.
- Meet with users and assist with creation of requirements packages.
- Recommend configuration management changes that will enhance system performance.
- Perform Systems Analysis by gathering high-level functional requirements, documenting results and findings, recommending course of action.
- Provide System Development Life Cycle support for web services, various portal products and services, software baselines, commercial-of-the-shelf (COTS) and Government-of-the-shelf (GOTS) software
- Complete a comprehensive, multi-disciplinary security assessment, addressing both content and technical issues at least annually on all web servers.
- Notify Customers within 10 workdays after they submit a request for a new capability.

3.7 TASK AREA 7 – BUSINESS PROCESS IMPROVEMENTS